JOURNAL OF ALGEBRA 70, 527–547 (1981)

The Cofree Irreducible Hopf Algebra on a Separable Field Extension

DAVID E. RADFORD*

Department of Mathematics, University of Illinois, Circle Campus, Chicago, Illinois 60680

Communicated by I. N. Herstein

Received January 29, 1979

0. INTRODUCTION

The purpose of this paper is to continue the study begun in [3] of to what extent the cofree irreducible Hopf algebra $\mathrm{CH}(U)$ on a commutative algebra U over a field k of characteristic $p > 0$ is determined by the restricted Lie (Frobenius) structure $\mathscr{L}(U)$ derived from the associative structure of U ($[u, v] = 0$ and $u^{[p]} = u^p$ for $u, v \in U$). Suppose U is a commutative algebra over a field k. If the characteristic of k is 0, then $\mathrm{CH}(U) \simeq \mathrm{Sh}(U)$, where $\mathrm{Sh}(U)$ is the shuffle algebra on the space U, by [3, Theorem 1.12]. Thus $\mathscr{L}(U)$ determines $\mathrm{CH}(U)$ whenever U is a commutative algebra in characteristic 0. $\mathscr{L}(U)$ determines $\mathrm{CH}(U)$ when U is nilpotent and k is a perfect field of characteristic $p > 0$ [3, Corollary 3.8]. In this paper we lay the foundation for the study of the cofree irreducible Hopf algebra $\mathrm{CH}(U)$ on a finite-dimensional separable algebra U over a field k of characteristic $p > 0$, concentrating on the fundamental case where U is a separable field extension. The first main result of this paper (Theorem 3.4) is that $\mathscr{L}(E)$ does not generally determine $\mathrm{CH}(E)$ when E is a finite-dimensional separable extension of k. The second main result (Theorem 3.6) gives a sufficient condition for $\mathscr{L}(E)$ to determine $\mathrm{CH}(E)$.

In Section 1 we analyze the structure of $\mathrm{CH}(U)$ when U is a finite-dimensional commutative algebra over a field k of characteristic $p > 0$ such that $U \otimes_k \Omega$ is split (meaning spanned by idempotents) for some Galois extension Ω of k. In this case $\mathrm{CH}(U) \otimes_k \Omega$ is split, and the standard results on forms of finite-dimensional algebras are used to determine the prime ideal structure of $\mathrm{CH}(U)$.

In Section 2 we examine in great detail the Lie structure $\mathscr{L}(E)$ of a finite-dimensional separable extension E of a field k of characteristic $p > 0$. $\mathscr{L}(E)$

* The research for this paper was partially supported by NSF Grant MCS77-00113 A01.

0021-8693/81/060527-21$02.00/0

determines the splitting field Ω of E over k, but generally does not determine E. More precisely, we show that $\mathscr{L}(E)$ determines E if $[E:k] \leqslant 6$, but not necessarily if $[E:k] = 7$. It is not hard to describe, in terms of the Galois group $G(\Omega\backslash k)$ of Ω over k, the isomorphism classes of (separable) field extensions of k with the same Lie structure as E. It is interesting to observe that if F is a finite-dimensional purely inseparable extension of k, then $\mathscr{L}(F)$ determines F as an algebra.

In Section 3 we prove the main results cited above. Additionally we show that the cofree irreducible Hopf algebra $\mathrm{CH}(E)$ on a finite-dimensional separable extension of k does not generally determine E as a separable extension. Again it is interesting to note that if F is a finite-dimensional purely inseparable extension of k, then $\mathscr{L}(F)$ determines $\mathrm{CH}(F)$ and $\mathrm{CH}(F)$ determines F as an algebra. We hope that our computational approach will shed light on the relationship between $\mathscr{L}(E)$ and $\mathrm{CH}(E)$ for finite-dimensional separable extensions E, and more generally the structure of $\mathrm{CH}(U)$ where U is a finite-dimensional separable algebra over k.

Our notations and conventions will follow [3, 6].

1. Forms of $\mathrm{CH}(U)$

Suppose that U is a commutative algebra (with unity) over a field k. We call U *split* if U is spanned by idempotents. In this section we shall be concerned with the structure of $\mathrm{CH}(U)$ when $U \otimes_k \Omega$ is split, where the characteristic of k is $p > 0$ and Ω is a Galois extension of k. The proof of the first lemma is straightforward and therefore is left to the reader.

1.1. Lemma. *Let U be a finite-dimensional commutative algebra over a field k of characteristic $p > 0$.*

(a) *U is split if and only if the roots of $X^p - X$ in U generate U.*

(b) *If U is split, then U has a unique basis $\mathscr{E}$ which is a set of orthogonal idempotents. ($\mathscr{E}$ is called the orthogonal basis of U.)*

(c) *Suppose U is split and V is an algebra over k. Then $\mathscr{L}(U) \simeq \mathscr{L}(V)$ implies $U \simeq V$. (Thus $\mathscr{L}(U)$ determines U as an algebra.)*

A subset $X = \{x_1, \ldots, x_s\}$ of a finite-dimensional commutative algebra U over a field k of characteristic $p > 0$ is said to be a *p-basis* if the monomials $x_1^{n_1} \cdot \cdots \cdot x_s^{n_s}$, where $0 \leqslant n_i < p$ for all i, form a linear basis for U. If $Y \subseteq U$ is a finite subset, and $f: Y \to Z_p$ is a function, set $e(f) = (-1)^{|Y|} \prod_{x \in Y}((x - f(x)) + \cdots + (x - f(x))^{p-1})$. If X is a p-basis for U and $x^p - x = 0$ for all $x \in X$, for each $f \in \mathrm{Map}(X, Z_p)$ let $\eta_f \in \mathrm{Alg}_k(U, k)$ be the algebra homomorphism determined by $\eta_f(x) = 1 + f(x)$ for $x \in X$. If U is a

finite-dimensional commutative split algebra over k and $e \in \mathscr{E}$, let $e^{\perp} \subseteq U$ be the maximal ideal generated by $1 - e$.

1.2. LEMMA. *Suppose U is a finite-dimensional commutative algebra over a field of characteristic $p > 0$ and X is a p-basis for U such that $x^p - x = 0$ for $x \in X$. Then U is split and*

(a) *The $e(f)$'s, where $f \in \mathrm{Map}(X, Z_p)$, constitute $\mathscr{E}$.*

(b) *$\eta_f(e(f')) = \delta_{f,f'}$ for $f, f' \in \mathrm{Map}(X, Z_p)$. In particular $\ker \eta_f = e(f)^{\perp}$.*

(c) *Let $Y \subseteq X$ be a non-void subset and $f_0 \in \mathrm{Map}(Y, Z_p)$. Then $e(f_0)$ is an idempotent, and $e(f_0) = \sum'_f e(f)$, where $f \in \mathrm{Map}(X, Z_p)$ runs over all extensions of f_0.*

Proof. Let $\alpha \in Z_p$. Then $\alpha + \cdots + \alpha^{p-1} = 0$ if $\alpha \neq 1$ and $= -1$ if $\alpha \neq 1$. Thus if $Y \subseteq X$ is any non-void subset and $f_0 \in \mathrm{Map}(Y, Z_p)$, then $\eta_f(e(f_0)) = \delta_{f_0, f|_Y}$. Since the η_f's constitute $\mathrm{Alg}_k(U, k)$, we have (a) and (b); and (c) now follows using the observation that $u = \sum_f \eta_f(u)\, e(f)$ for $u \in U$. Q.E.D.

Now suppose that U is any algebra over a field k and F is a field extension of k. The Galois group $G(F\backslash k)$ acts faithfully as k-algebra automorphisms on $U \otimes {}_kF$ ($\sigma \cdot (u \otimes \alpha) = u \otimes \sigma(\alpha)$). We may consider U as a k-subalgebra of $U \otimes {}_kF$ via the map $u \mapsto u \otimes 1$.

1.3. *Let U be an algebra over a field k, and suppose that F is a finite-dimensional extension of k.*

(a) *U is the set of $G(F\backslash k)$ fixed points of $U \otimes {}_kF$ if F is Galois.*

(b) *Assume that U is finite-dimensional, commutative, and $U \otimes {}_kF$ is split. Let $\mathscr{E}$ be the orthogonal basis of $U \otimes {}_kF$. Then $\sigma \cdot \mathscr{E} \subseteq \mathscr{E}$ for $\sigma \in G(F\backslash k)$. Thus the set $\mathscr{E}$ is a $G(F\backslash k)$-module.*

Suppose F is a field extension of k. For $S \subseteq G(F\backslash k)$ we denote by $S' \subseteq F$ the set of those $a \in F$ fixed by all $\sigma \in S$, and for $T \subseteq F$ we denote by $T' \subseteq G(F\backslash k)$ the set of $\sigma \in G(F\backslash k)$ which fix all $a \in T$. Now assume that F is Galois, U is a k-algebra, and that $U \otimes {}_kF$ has an orthogonal basis $\mathscr{E}$. Suppose $e \in \mathscr{E}$ and $\sigma_1, \ldots, \sigma_n \in G(F\backslash k)$ are representatives of the left cosets of the stabilizer $G(F\backslash k)_e$ of e. Let U_e be the set of sums $\sum_{i=1}^n \alpha_i(\alpha)\, \sigma_i \cdot e$, where $\alpha \in G(F\backslash k)'_e$. One can easily show that U_e does not depend on the choice of representatives, $U_e \subseteq U$, and that $U_e U_{e'} = (0)$ if $e' \notin G(F\backslash k) \cdot e$. Evidently $U_e \to G(F\backslash k)'_e$ ($\sum_{i=1}^n \sigma_i(\alpha)\, \sigma_i \cdot e \mapsto \alpha$) is an isomorphism of k-algebras. If X is a left G-module and $S \subseteq X$ is a subset, let $G_S = \{\sigma \in G : \sigma \cdot S \subseteq S\}$ denote the stabilizer of S.

1.4. PROPOSITION. *Let U be a finite-dimensional commutative algebra*

over a field k, Ω a Galois extension of k, and suppose $U \otimes {}_k\Omega$ has an orthogonal basis $\mathscr{E}$.

(a) *Let $e_1, \ldots, e_s \in \mathscr{E}$ be representatives of the $G(\Omega\backslash k)$-orbits of $\mathscr{E}$. Then $U = U_{e_1} \oplus \cdots \oplus U_{e_s}$ as algebras.*

(b) *For $e \in \mathscr{E}$, U_e is a minimal ideal of U, and $U_e \simeq G(\Omega\backslash k)'_e$ as algebras.*

(c) *Let $\mathscr{M} = e^{\perp}$ be a maximal ideal of $U \otimes {}_k\Omega$. Then $m = \bigcap_\sigma \sigma \cdot \mathscr{M}$, where σ runs over $G(\Omega\backslash k)$, is a maximal ideal of U, and $U/m \simeq G(\Omega\backslash k)'_e$. All prime ideals are maximal, and all maximal ideals m of U are of this form (so if $\mathscr{M} \subseteq U \otimes {}_k\Omega$ is a maximal ideal containing m, then $U/m \simeq G(\Omega\backslash k)'_{\mathscr{M}}$).*

Proof. If e and e' are not in the same $G(\Omega\backslash k)$-orbit, then $U_e U_{e'} = (0)$. It is clear that $U_{e_1} + \cdots + U_{e_s}$ is direct. Since $\dim U_e = [G'_e : k] = [G : G_e]$, where $G = G(\Omega\backslash k)$, we compute $\dim(U_{e_1} + \cdots + U_{e_s}) = [G : G_{e_1}] + \cdots + [G : G_{e_s}] = |\mathscr{E}| = \dim U$. Thus (a) follows. Since $U_e \simeq G(\Omega\backslash k)'_e$ we now have (b). To show (c) note $e \in G(\Omega\backslash k) \cdot e_i$ for some i. By 1.3(a) $\bigcap_\sigma \sigma \cdot \mathscr{M}$ is an ideal of U. Now $I = U_{e_1} + \cdots + \hat{U}_{e_i} + \cdots + U_{e_s} \subseteq e^{\perp}$, so $I \subseteq \bigcap \sigma \cdot \mathscr{M}$. But I is a maximal ideal of U by (b), so $m = I$ and $U/m \simeq U_{e_i}$. Now (c) follows easily. Q.E.D.

Let U be a finite-dimensional commutative algebra over a field k of characteristic $p > 0$. Then the cofree irreducible Hopf algebra $\mathrm{CH}(U)$ on U is commutative and the (Hopf) subalgebra $\langle \mathrm{CH}(U)_n \rangle$ generated by the nth term of the coradical filtration $\mathrm{CH}(U)_n$ of $\mathrm{CH}(U)$ is finite-dimensional [3, Proposition 1.5a) and Corollary 1.6a)]. The important fact about the pth powers in $\mathrm{CH}(U)$ is:

1.5. [3, Proposition 1.5b)]. *Let U be a commutative algebra over a field of characteristic $p > 0$ and $u_1, \ldots, u_n \in U$. Then $(u_1 \otimes \cdots \otimes u_n)^p = u_1^p \otimes \cdots \otimes u_n^p$ (the former multiplication in $\mathrm{CH}(U)$ and the latter multiplications in U). In particular u^p is unambiguous for $u \in U$.*

Since $\langle \mathrm{CH}(U)_1 \rangle \subseteq \langle \mathrm{CH}(U)_2 \rangle \subseteq \cdots \subseteq \bigcup_{n=1}^{\infty} \langle \mathrm{CH}(U)_n \rangle = \mathrm{CH}(U)$ in any case, and $\mathrm{CH}(U)_n$ is spanned by tensors of the form $u_1 \otimes \cdots \otimes u_m$, where $m \leqslant n$ and $u_1, \ldots, u_m \in \mathscr{E}$ in the split case, we also use Lemma 1.1 to deduce:

1.6. PROPOSITION. *Let U be a finite-dimensional commutative split algebra over a field k of characteristic $p > 0$. Then $\mathrm{CH}(U)$ is commutative and*

(a) *For each $n \geqslant 1$ the subHopf algebra $\langle \mathrm{CH}(U)_n \rangle$ is finite-dimensional and split.*

(b) *Let $\mathscr{M} \subseteq \mathrm{CH}(U)$ be a maximal ideal. Then $\mathscr{M} \cap \langle \mathrm{CH}(U)_n \rangle$ is a maximal ideal of $\langle \mathrm{CH}(U)_n \rangle$ for all $n \geqslant 0$.*

Now assume U is split and has orthogonal basis $\mathscr{E} = \{u_1,..., u_r\}$. Regard $[r] \equiv \{1,..., r\}$ as a well-ordered set in the natural way, let S be the free semigroup generated by $[r]$, and let $\mathscr{P} \subseteq S$ be the p-adic primes of S [3, §2; 5, §2]. For $\mathscr{p} = i_1 \cdot \cdots \cdot i_s \in S$ $(1 \leqslant i_j \leqslant r)$ let $u_{\mathscr{p}} = u_{i_1} \otimes \cdots \otimes u_{i_s}$, $|\mathscr{p}| = s$ denote the length of $\mathscr{p}$, and let $\mathscr{P}_{n,\mathscr{E}} = \{\mathscr{p} \in \mathscr{P} : |\mathscr{p}| \leqslant n\}$. We can give an explicit description of the orthogonal basis of $\langle \mathrm{CH}(U)_n \rangle$ in terms of $\mathscr{E}$.

1.7. PROPOSITION. *Let U be a finite-dimensional commutative split algebra over a field k of characteristic $p > 0$, let $\mathscr{E} = \{u_1,..., u_r\}$ be the orthogonal basis for U, let S be the free semigroup generated by $[r]$, and let $\mathscr{P}$ be the p-adic primes of S.*

(a) *The $u_{\mathscr{p}}$'s, where $\mathscr{p} \in \mathscr{P}_{n,\mathscr{E}}$, form a p-basis for $\langle \mathrm{CH}(U)_n \rangle$, and $u_{\mathscr{p}}^p - u_{\mathscr{p}} = 0$ for $\mathscr{p} \in \mathscr{P}_{n,\mathscr{E}} = \mathscr{P}_n$ (hence $\langle \dim \mathrm{CH}(U)_n \rangle = p^{|\mathscr{P}_n|}$).*

(b) *The orthogonal basis $\mathscr{E}_n$ for $\langle \mathrm{CH}(U)_n \rangle$ consists of the $e(f) = (-1)^{|\mathscr{P}_n|} \prod_{\mathscr{p} \in \mathscr{P}_n} ((u_{\mathscr{p}} - f(u_{\mathscr{p}})) + \cdots + (u_{\mathscr{p}} - f(u_{\mathscr{p}}))^{p-1})'$s, where $f \in \mathrm{Map}(\mathscr{P}_{n,\mathscr{E}}, Z_p)$.*

(c) *Suppose $m < n$ and $e(f_0) \in \mathscr{E}_m$. Then $e(f_0) = \sum_f' e(f)$, where $f \in \mathrm{Map}(\mathscr{P}_{n,\mathscr{E}}, Z_p)$ runs over all extensions of f_0.*

Proof. That the $u_{\mathscr{p}}$'s, where $\mathscr{p} \in \mathscr{P}_n$, form a p-basis for $\langle \mathrm{CH}(U)_n \rangle$ is [3, Corollary 2.5]. By 1.5, $u_{\mathscr{p}}^p = u_{\mathscr{p}}$ for $\mathscr{p} \in \mathscr{P}$. The rest follows now by Lemma 1.2. Q.E.D.

1.8. *If U is any algebra over a field k, then $u \cdot v = u \otimes v + v \otimes u + uv$ for $u, v \in U$ ($\cdot$ denotes multiplication in $\mathrm{CH}(U)$ and juxtaposition denotes multiplication in U).*

The above follows by the remark immediately after [3, Lemma 1.11].

Remark. Let U be any algebra over a field k and $u \in U$ be a non-zero idempotent of U. Then u is an idempotent of $\mathrm{CH}(U)$ if and only if $\mathrm{char}\, k = 2$. In particular, idempotents of U are *not* generally idempotents of $\mathrm{CH}(U)$.

Let U be any algebra over a field k and suppose σ is an algebra automorphism of U. Then by the universal mapping property of the cofree irreducible Hopf algebra $(\mathrm{CH}(U), \pi)$ on U [3, Theorem 1.4] there is a unique Hopf algebra automorphism $\boldsymbol{\sigma}$ on $\mathrm{CH}(U)$ such that the diagram

$$\begin{array}{ccc} \mathrm{CH}(U)^+ & \xrightarrow{\boldsymbol{\sigma}} & \mathrm{CH}(U)^+ \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ U & \xrightarrow{\sigma} & U \end{array} \quad \text{commutes.}$$

$\boldsymbol{\sigma}(u_1 \otimes \cdots \otimes u_n) = \sigma(u_1) \otimes \cdots \otimes \sigma(u_n)$ for $u_1,..., u_n \in U$ since this describes

the only coalgebra map making the diagram commute. Thus $\mathfrak{F} = \mathrm{Aut}_k(U)$ acts as Hopf algebra automorphisms on $\mathrm{CH}(U)$ ($\sigma \cdot h = \sigma(h)$ for $\sigma \in \mathfrak{F}$ and $h \in \mathrm{CH}(U)$). Hence if U is finite-dimensional and commutative, and F is a finite-dimensional extension of k such that $U \otimes {}_kF$ is split, then by virtue of 1.3(b) we conclude that $\sigma \in G(F\backslash k)$ acts as a Hopf algebra automorphism on $\mathrm{CH}(U \otimes {}_kF)$ ($e \mapsto \sigma \cdot e$ for $e \in \mathscr{E}$).

Now assume F is a field extension of k. Then $(\mathrm{CH}(U) \otimes {}_kF,\ \pi \otimes I)$ is easily seen to be the cofree irreducible Hopf algebra on $U \otimes {}_kF$. Notice that the canonical isomorphism $\mathrm{CH}(U) \otimes {}_kF \to \mathrm{CH}(U \otimes {}_kF)$ is determined by $(u_1 \otimes \cdots \otimes u_n) \otimes \alpha \mapsto (u_1 \otimes 1) \otimes \cdots \otimes (u_n \otimes \alpha)$, where $u_1, \ldots, u_n \in U$ and $\alpha \in F$.

Suppose that A is an algebra defined over a field F, $k \subseteq F$ is a subfield of F, and $G \subseteq G(F\backslash k)$ is a subgroup which gives A a (left) G-module structure. Then A is called a *G-module algebra* if for all $\sigma \in G$ left translation $\sigma \cdot$ by σ on A is a σ-linear k-algebra automorphism. A bialgebra A is called a *G-module* bialgebra if A is a G-module algebra, and in addition $\Delta\sigma \cdot a = \sum \sigma \cdot a_{(1)} \otimes \sigma \cdot a_{(2)}$ and $\varepsilon(\sigma \cdot a) = \sigma(\varepsilon(a))$ hold for $\sigma \in G$ and $a \in A$. Observe that if A is a bialgebra defined over a field k, and F is any extension of k, then $A \otimes {}_kF$ is a $G(F\backslash k)$-module bialgebra ($\sigma \cdot (a \otimes \alpha) = a \otimes \sigma(\alpha)$).

1.9. LEMMA. *Let A be a finite-dimensional commutative split bialgebra over a field F of characteristic $p > 0$, let k be a subfield of F, and let $G \subseteq G(F\backslash k)$ be a subgroup. Suppose A is a G-module bialgebra and $\mathscr{E}$ is the orthogonal basis of A. Then for $\sigma \in G$, the correspondence $e \mapsto \sigma \cdot e$, where $e \in \mathscr{E}$, determines a (unique) bialgebra automorphism of A.*

Proof. Since $\sigma \cdot$ is a ring automorphism, it follows that $\sigma \cdot \mathscr{E} \subseteq \mathscr{E}$. Thus $\sigma \cdot$ permutes $\mathscr{E}$. Let $\mathscr{E} = \{e_1, \ldots, e_n\}$. Then the $e_i \otimes e_j$'s constitute an orthogonal idempotent basis for $A \otimes {}_FA$. For $e \in \mathscr{E}$, Δe is an idempotent of $A \otimes {}_FA$, so $\Delta e = \sum \alpha_{i,j} e_i \otimes e_j$, where $\alpha_{i,j} = 0$ or 1. This means $\Delta\sigma \cdot e = \sum \alpha_{ij} \sigma \cdot e_i \otimes \sigma \cdot e_j$ for $\sigma \in G(\Omega\backslash k)$. Now it is clear that the F-linear extension of $\sigma \cdot |_{\mathscr{E}}$ is a bialgebra automorphism. Q.E.D.

1.10 PROPOSITION. *Let U be a finite-dimensional commutative algebra over a field k of characteristic $p > 0$, and suppose F is a finite-dimensional extension of k such that $U \otimes {}_kF$ is split. Then*:

(a) *$\langle \mathrm{CH}(U)_n \rangle \otimes {}_kF$ is finite-dimensional and split for $n \geqslant 1$.*

(b) *The action of $G(F\backslash k)$ on the orthogonal set $\mathscr{E}$ of $\langle \mathrm{CH}(U)_n \rangle \otimes {}_kF$ described in* 1.3(b) *extends linearly to an action by Hopf algebra automorphisms. If $m \leqslant n$, then this automorphism action of $G(F\backslash k)$ on $\langle \mathrm{CH}(U)_n \rangle \otimes {}_kF$ extends that on $\langle \mathrm{CH}(U)_m \rangle \otimes {}_kF$. Thus $G(F\backslash k)$ acts in a unique way as Hopf algebra automorphisms of $\mathrm{CH}(U) \otimes {}_kF$ such that the action extends that on $\langle \mathrm{CH}(U)_n \rangle \otimes {}_kF$ for $n \geqslant 1$.*

(c) *The canonical isomorphism* $\mathrm{CH}(U) \otimes {}_kF \simeq \mathrm{CH}(U \otimes {}_kF)$ *is an isomorphism of* $G(F\backslash k)$*-modules* ($G(F\backslash k)$ *acting as Hopf algebra automorphisms in both cases*).

Proof. (a) $\langle \mathrm{CH}(U)_n \rangle \otimes {}_kF \simeq \langle (\mathrm{CH}(U \otimes {}_kF))_n \rangle$ under the canonical isomorphism, so (a) follows by Proposition 1.6(a).

(b) The action of $G(F\backslash k)$ on $\langle \mathrm{CH}(U)_n \rangle \otimes {}_kF$ is by bialgebra (hence Hopf) algebra automorphisms by 1.9. The remainder follows now using the fact

$$\langle \mathrm{CH}(U)_1 \rangle \otimes {}_kF \subseteq \langle \mathrm{CH}(U)_2 \rangle \otimes {}_kF$$

$$\subseteq \cdots \subseteq \bigcup_{n=1}^{\infty} \langle \mathrm{CH}(U)_n \rangle \otimes {}_kF = \mathrm{CH}(U) \otimes {}_kF.$$

(c) We need only show that if $\sigma \in G(F\backslash k)$ and $\mathscr{O}$ is the Hopf algebra automorphism of $\mathrm{CH}(U) \otimes {}_kF$ describing the action of σ, then the diagram

$$\begin{array}{ccc} \mathrm{CH}(U)^+ \otimes {}_kF & \xrightarrow{\mathscr{O}} & \mathrm{CH}(U)^+ \otimes {}_kF \\ \downarrow{\scriptstyle \pi \otimes I} & & \downarrow{\scriptstyle \pi \otimes I} \\ U \otimes {}_kF & \xrightarrow{\tilde{\sigma} \cdot} & U \otimes {}_kF \end{array}$$

commutes, where $\tilde{\sigma} \cdot$ is the F-linear extension of $\sigma \cdot$ restricted to the orthogonal basis $\mathscr{E}$ of $U \otimes {}_kF$. But as $(\tilde{\sigma} \cdot)(\mathbf{u}) = \sigma \cdot \mathbf{u}$ for any idempotent $\mathbf{u} \in U \otimes {}_kF$, it is easy to see that $(\tilde{\sigma} \cdot) \circ (\pi \otimes I) \equiv (\pi \otimes I) \circ \mathscr{O}$ on idempotents of $\mathrm{CH}(U)^+ \otimes {}_kF$, i.e., a spanning set of $\mathrm{CH}(U)^+ \otimes {}_kF$. Thus the diagram commutes. Q.E.D.

1.11. PROPOSITION. *Let* U *be a finite-dimensional commutative algebra over a field* k *of characteristic* $p > 0$.

(a) *Prime ideals of* $\mathrm{CH}(U)$ *are maximal.*

(b) *Let* $m \subseteq \mathrm{CH}(U)$ *be a maximal ideal. Then* $m \cap \langle \mathrm{CH}(U)_n \rangle$ *is a maxial ideal of* $\langle \mathrm{CH}(U)_n \rangle$ *for* $n \geqslant 1$. *Any maximal ideal* m_0 *of* $\langle \mathrm{CH}(U)_n \rangle$ *can be extended to a maximal ideal* m *of* $\mathrm{CH}(U)$.

(c) *Suppose* Ω *is a Galois extension of* k *such that* $U \otimes {}_k\Omega$ *is split. Let* m *be a maximal ideal of* $\mathrm{CH}(U)$ *and* $\mathscr{M}$ *a maximal ideal of* $\mathrm{CH}(U) \otimes {}_k\Omega$ *such that* $m \subseteq \mathscr{M}$. *Then* $\mathrm{CH}(U)/m \simeq G(\Omega\backslash k)'\mathscr{M}$.

Proof. (a) and (b). $A_n = \langle \mathrm{CH}(U)_n \rangle$ is a finite-dimensional commutative algebra and $A_1 \subseteq A_2 \subseteq \cdots \subseteq \bigcup A_n = A$. (c) follows by the canonical identifications $\mathrm{CH}(U) \otimes {}_k\Omega \simeq \mathrm{CH}(U \otimes {}_k\Omega)$ and $\langle \mathrm{CH}(U)_n \rangle \otimes {}_k\Omega \simeq \langle \mathrm{CH}(U \otimes {}_k\Omega)_n \rangle$ for $n \geqslant 1$, Propositions 1.6, 1.10b), and 1.4c). Q.E.D.

Let U be a commutative algebra over a field k of characteristic $p > 0$. A subalgebra $V \subseteq U$ is called separable if $V \otimes_k$ is spanned by idempotents

(or equivalently is generated by its roots of $X^p - X$), where $\bar{k}$ is an algebraic closure of k. U has a unique maximal separable subalgebra U_{sep} which is characterized by $U_{\text{sep}} \otimes_k \bar{k} = (U \otimes_k \bar{k})_{\text{sep}}$. In particular U_{sep} is the sum of all separable subalgebras of U. If U' is also a commutative algebra over k and $f: U \to U'$ is a restricted Lie map, then clearly $f(U_{\text{sep}}) \subseteq U'_{\text{sep}}$. The functor $(\ )_{\text{sep}}$ commutes with tensor product, so if A is a commutative bialgebra (resp., Hopf algebra) over k, then A_{sep} is a subbialgebra (resp., sub-Hopf algebra) of A. The last result of this section shows that $(\ )_{\text{sep}}$ commutes with CH( ) as well.

1.12. THEOREM. *Let U be a commutative algebra over a field k of characteristic $p > 0$. The inclusion $U_{\text{sep}} \subsetneq U$ induces an isomorphism of Hopf algebras* $\text{CH}(U_{\text{sep}}) \simeq \text{CH}(U)_{\text{sep}}$.

Proof. $(\text{CH}(U)_{\text{sep}}) \otimes_k \bar{k} \simeq \text{CH}(U_{\text{sep}} \otimes_k \bar{k})$ means $\text{CH}(U_{\text{sep}})$ is separable by Proposition 1.6(a). Let $(\text{CH}(U_{\text{sep}}), \pi)$ and $(\text{CH}(U), \pi)$ be the cofree irreducible Hopf algebras on U_{sep} and U, respectively. It is easy to see that $(\text{CH}(U_{\text{sep}}), \pi)$ and $(\text{CH}(U)_{\text{sep}}, \pi_{\text{sep}})$ are both the cofree irreducible commutative separable Hopf algebra on U_{sep}. Q.E.D.

2. THE LIE STRUCTURE OF A SEPARABLE FIELD EXTENSION E

In this section we determine what it means for two finite-dimensional separable extensions of a field k of characteristic $p > 0$ to have the same Lie (Frobenius) structure. The Lie structure $\mathscr{L}(E)$ determines the splitting field Ω of E over k, but generally not E. Thus the problem of determining which extensions F have the same Lie structure as E reduces to considering subfields of Ω.

We will first consider Lie properties of finite-dimensional field extensions. As might be expected, the minimal p-polynomial of $x \in F$ is the basic concept in our study.

2.1. *Let F be a finite-dimensional extension of a field k of characteristic $p > 0$. Then $x \in F$ is separable if and only if the minimal p-polynomial of x over k has the form $f(X) = \alpha_0 X + \alpha_1 X^p + \cdots + X^{p^n}$, where $\alpha_0 \neq 0$.*

Proof. ($\Leftarrow$) Let $p = p(X)$ be the minimal polynomial of x over k. Then $pq = f(X)$ for some $q \in k[X]$. Taking the derivative of both sides we compute $p'q + pq' = \alpha_0$, so $p' \neq 0$. This means x is separable [2, Theorem 23, p. 25].

($\Rightarrow$) Assume x is separable and suppose $f(X) = \alpha_0 X + \cdots + X^{p^n}$ is the minimal p-polynomial of x over k. Now $x, x^p, \ldots, x^{p^{n-1}}$ are independent, so $x^p, x^{p^2}, \ldots, x^{p^n}$ are also since x is separable [1, Chap. V, Sect. 8, No. 2, Corollary to Proposition 3]. Thus $\alpha_0 \neq 0$. Q.E.D.

2.2. LEMMA. *Let k be a field of characteristic $p > 0$ and suppose $f: F \to U$ is a restricted Lie isomorphism, where F is a finite-dimensional field extension of k and U is a k-algebra.*

(a) *f preserves the prime field Z_p of k, so $f(k) = k \cdot 1$.*

(b) *For a non-zero $\alpha \in Z_p$ the map defined by $x \mapsto \alpha \sum(x)$ is a Lie isomorphism. (Thus there is a Lie isomorphism $f': F \to U$ with $f'(a) = a \cdot 1$ for $a \in k$.)*

(c) *U is a field, and $x \in F$ is separable (resp., purely inseparable) over k if and only if $f(x)$ is separable (resp., purely inseparable) over k.*

(d) *If F is a purely inseparable extension, then $\mathscr{L}(F)$ determines F as a k-algebra.*

Proof. (a) Since the prime field of F consists of the roots of $X^p - X$, f preserves Z_p. This means $f(1) \in k \cdot 1$, whence $f(k) = k \cdot 1$. To show (b) notice that f' is the composite of the Lie automorphism of U determined by $a \to \alpha a$ (U must be commutative) and f. The parenthetical remark now follows by (a) where $f(\alpha) = 1$. To show that U is a field we may assume $f(1) = 1$ by (b). We have noted U is commutative. U has no non-zero nilpotent elements and one idempotent. Thus U is a field. The remainder of (c) easily follows. (d) follows from (c) and the realization that both F and U are splitting fields of a family of polynomials of the form $X^{p^n} - a$, where $a \in k$. Q.E.D.

The key to the Lie structure of a finite-dimensional separable extension E of degree n over an infinite field k of characteristic $p > 0$ is the existence of an $u \in E$ such that the pth powers $u, u^p, \ldots, u^{p^{n-1}}$ of u form a linear basis for E over k. (This is equivalent to saying that $\mathscr{L}(E)$ is principal.) The proof we give is based on the following lemma.

2.3. LEMMA. *Let F be an extension of an infinite field k of characteristic $p > 0$ and suppose $a_1, \ldots, a_n \in F$ are distinct. There are $\alpha_0, \ldots, \alpha_{n-1} \in k$ such that the $u_i = \alpha_0 1 + \alpha_1 a_i + \cdots \alpha_{n-1} a_i^{n-1}$'s $(1 \leqslant i \leqslant n)$ are independent over Z_p.*

Proof. Let

$$A = \begin{bmatrix} 1 & a_1 \cdots a_1^{n-1} \\ \vdots & \\ 1 & a_n \cdots a_n^{n-1} \end{bmatrix}.$$

Then $\det A = \prod_{i<j}(a_j - a_i)$, so A is invertible. The $(x_1, \ldots, x_n)A$'s, where $x_i \in Z_p$, form a finite set $S \subseteq F^n$. Since k is infinite, by induction on n it is easy to see there exist $\alpha_0, \ldots, \alpha_{n-1} \in k$ such that for $(s_1, \ldots, s_n) \in S$ the relation $\sum_{i=1}^{n} \alpha_{i-1} s_i = 0$ implies $s_1 = \cdots = s_n = 0$. Set $u_i = \alpha_0 1 +$

$\alpha_1 a_i + \cdots + \alpha_{n-1} a_i^{n-1}$. Then for $(s_1,..., s_n) = (x_1,..., x_n)A \in S$ we compute $\sum_{i=1}^n x_i u_i = \sum_{i=1}^n \alpha_{i-1} s_i$. Thus since A is invertible, the relation $\sum_{i=1}^n x_i u_i = 0$, where $x_1,..., x_n \in Z_p$, implies $x_1 = \cdots = x_n = 0$. Q.E.D.

For the reader's convenience we will derive the characterization of p-polynomial which will be needed in the proof of Proposition 2.5.

2.4. *Suppose $f(X) \in k[X]$ splits into distinct linear factors over k, where k is field of characteristic $p > 0$. Then the following are equivalent:*

(a) $f(X) = \alpha_0 X + \alpha_1 X^p + \cdots + \alpha_n X^{p^n}$ *for some* $\alpha_0,..., \alpha_n \in k$.

(b) *The roots V of $f(X)$ form an additive subgroup.*

(c) $f(X + Y) = f(X) + f(Y)$, *viewing f as a polynomial over $k[X, Y]$.*

Proof. (a) $\Rightarrow$ (b) is clear. To show (b) $\Rightarrow$ (c) observe that $f(X + v) = f(X)$ for $v \in V$, so $d(Y) = f(X + Y) - f(X) - f(Y) \in k(X)[Y]$ vanishes on V. Hence $d(Y) = 0$ by degree considerations. We show (c) $\Rightarrow$ (a) in any case. $f(X) = \beta_1 X + \cdots + \beta_m X^m$ for some m where $\beta_m \neq 0$. Since $f(X) - \beta_1 X$ satisfies (c) we may assume $\beta_1 = 0$. Since the coefficient of $X^{i-1}Y$ in the expansion of $f(X + Y)$ is $i\beta_i$, we have $i\beta_i = 0$ for $1 < i \leqslant m$. Thus $\beta_i = 0$ unless $p \mid i$, so $f(X) = \beta_p(X^p) + \cdots + \beta_m(X^p)^{m/p} \equiv g(X^p)$. From $g(X^p + Y^p) = g(X^p) + g(Y^p)$ it follows that $g(X + Y) = g(X) + g(Y)$, so (c) $\Rightarrow$ (a) is proved by induction on $\deg f(X)$. Q.E.D.

For a field extension $k \subseteq \Omega$ and $u \in \Omega$ let $V(u, \Omega\backslash k)$ denote the additive subgroup generated by $G(\Omega\backslash k)(u)$ (the conjugates of u in Ω).

2.5. PROPOSITION. *Let E be an n-dimensional separable extension of an infinite field k of characteristic $p > 0$, and let Ω be a splitting field of E over k.*

(a) *For $u \in \Omega$ the minimal p-polynomial of u over k is* $f(X) = \prod_{v \in V(u, \Omega\backslash k)} (X - v)$.

(b) *If $E = k[u]$ then following are equivalent:*

(i) *$\mathscr{L}(E)$ is generated by u (or equivalently $u, u^p,..., u^{p^{n-1}}$ is a basis for E over k).*

(ii) *The minimal p-polynomial of u over k has the form* $f(X) = \alpha_0 X + \cdots + X^{p^n}$.

(iii) *$V(u, \Omega\backslash k)$ has p^n elements (or equivalently* $\dim_{Z_p} V(u, \Omega\backslash k) = n$).

(iv) *$G(\Omega\backslash k)(u)$ is a basis for $V(u, \Omega\backslash k)$ as a vector space over Z_p.*

(c) *$\mathscr{L}(E)$ is principal.*

Proof. (a) Let $f(X)$ be the minimal p-polynomial of u over k. The roots of $f(X)$ form an additive subgroup, so any $v \in V(u, \Omega\backslash k)$ is a root of $f(X)$. Since $V(u, \Omega\backslash k)$ is stable under $G(\Omega\backslash k)$, $\prod_v (X - v) \in k[X]$, so (a) follows. (b) is straightforward. To show (c) write $E = k[a]$ for some $a \in E$. Since k is infinite, by Lemma 2.3 there are $\alpha_0, \ldots, \alpha_{n-1} \in k$ such that the $u_i = \alpha_0 1 + \alpha_1 a_i + \cdots + \alpha_{n-1} a_i^{n-1}$'s for $1 \leqslant i \leqslant n$ are independent over Z_p, where $a_i, \ldots, a_n \in \Omega$ are the conjugates of a. As the u_i's are the conjugates of $u = \alpha_0 a + \cdots + \alpha_{n-1} a^{n-1}$, (c) now follows from (b). Q.E.D.

2.6. PROPOSITION. *Let E, F be finite-dimensional separable extensions of a field k of characteristic $p > 0$, and suppose Ω_E, Ω_F are splitting fields of E, F, respectively, over k. Then $\mathscr{L}(E) \simeq \mathscr{L}(F)$ implies $\Omega_E \simeq \Omega_F$ as fields. (Thus $\mathscr{L}(E)$ determines E as an algebra if E is a Galois extension.)*

Proof. If k is finite the conclusion is clear; if k is infinite we apply the preceding proposition. The paranthetical remark now follows by Lemma 2.2. Q.E.D.

Let E be a finite-dimensional separable extension of an infinite field k of characteristic $p > 0$, and suppose Ω is a splitting field of E over k. By virtue of the preceding proposition and Lemma 2.2 the problem of finding the algebras with the same Lie structure as E is the problem of finding the isomorphism classes of the subfields of Ω with the same Lie structure.

2.7. THEOREM. *Let E be a finite-dimensional separable extension of an infinite field k of characteristic $p > 0$, and suppose Ω is a splitting field of E over k. Let $u \in E$ generate $\mathscr{L}(E)$.*

(a) *For a field extension $k \subseteq F \subseteq \Omega$, $\mathscr{L}(E) \simeq \mathscr{L}(F)$ if and only if $F = k[\omega]$, where $\omega \in V(u, \Omega\backslash k)$ and $G(\Omega\backslash k)(\omega)$ is a basis for $V(u, \Omega\backslash k)$ over Z_p (such a ω is called a $G(\Omega\backslash k)$-orbit basis generator).*

(b) *The number of isomorphism classes of k-algebras with restricted Lie structure isomorphic to $\mathscr{L}(E)$ is the number of conjugacy classes of the $G(\Omega\backslash k)_\omega$'s, where $\omega \in V(u, \Omega\backslash k)$ is a $G(\Omega\backslash k)$-orbit basis generator.*

Proof. (a) follows by Proposition 2.5. (b) follows by Lemma 2.2, the preceding proposition, and the fact that two extensions E, $F \subseteq \Omega$ of k are isomorphic if and only if E' and F' are conjugate. Q.E.D.

Using the last theorem we will show that $\mathscr{L}(E)$ determines E if E is a separable extension of a field k of characteristic $p > 0$ and $[E: k] \leqslant 6$. This is not the case in degree 7. We first abstract the setting of the preceding theorem.

Let k be any field and $G \subseteq \mathrm{Aut}_k(V)$ be a subgroup, where V is a finite-dimensional vector space over k. We call a subgroup $H \subseteq G$ *closed* if H is

the intersection of *point* stabilizers G_v. G and (e) are closed, and the intersection of closed subgroups is closed; in particular a subgroup $H \subseteq G$ is contained in a smallest closed subgroup which we denote by $\bar{H}$. Suppose $u \in V$ is a G-orbit basis generator (which means $G(u)$ is a basis for V). Then we may regard $G \subseteq \mathrm{Sym}(G(u))$ as a transitive subgroup of permutations of $G(u)$. It is easy to see that $H \subseteq G$ is closed if and only if H is the intersection of *set* stabilizers G_U where $U \subseteq G(u)$, and that $\bar{H} = \bigcap G_{\mathcal{O}}$ where $\mathcal{O}$ runs over the H-orbits of $G(u)$. We extend the notion of closed to groups $G \subseteq \mathrm{Sym}(X)$ in the obvious way. Regarding $G \subseteq \mathrm{Sym}(G(u))$ as a permutation group one can easily show:

2.8. LEMMA. *Let V be an n-dimensional vector space over a field k and let $G \subseteq \mathrm{Aut}_k(V)$ be a subgroup. Suppose u, $w \in V$ are G-orbit basis generators and $L \subseteq G$ is a subgroup.*

(a) $[G: G_u] = n$.

(b) $|G_u \cdot w| = [G_u: G_u \cap G_w] = [G_w: G_w \cap G_u] = |G_w \cdot u|$.

(c) *If $G_u \subseteq L$, then L is closed.*

(d) *If LG_u is a subgroup and is dense, then L is dense.*

(e) *If L is normal and $L \subseteq G_u$, then $L = (e)$.*

(f) *If L is a normal maximal closed subgroup, then $G_u \subseteq L$.*

(g) *Let $\tau \in \mathrm{Aut}_k(V)$. Then $\tau(u)$ is a ${}^{\tau}G$-orbit basis generator and* ${}^{\tau}(G_u) = ({}^{\tau}G)_{\tau(u)}$.

If (g) we are using the standard notation ${}^{\tau}a = \tau a \tau^{-1}$ for τ, $a \in G$ where G is any group. If $G = \mathrm{Sym}(X)$, we note that ${}^{\tau}(x_1, \ldots, x_n) = (\tau x_1, \ldots, \tau x_n)$ for cycles in G.

2.9 PROPOSITION. *Let k be any field and let $G \subseteq \mathrm{Aut}_k(V)$ be a subgroup, where V is an n-dimensional vector space over k.*

(a) *If $n \leqslant 6$, then the stabilizers G_u of G-orbit basis generators are all conjugate.*

(b) *If $n = 7$, there is more than one conjugacy class of stabilizers G_u of G-orbit basis generators if and only if* char $k \neq 2$ *and $G \simeq GL_3(Z_2)$. In this case there are two such conjugacy classes.*

Proof. Suppose u, $w \in V$ are G-orbit basis generators and let $X = G(u)$. We will regard $G \subseteq \mathrm{Sym}(X)$ concretely as a transitive permutation group and consider the various possibilities for the G_w-orbits of X. Observe that the conjugates of G_u are the G_x's for $x \in X$. The next two results will take care of the cases $n \leqslant 6$.

2.10. (a) *If $G = S_n$ or A_n, then all non-transitive index n subgroups are conjugate.*

(b) *Suppose $G \subseteq S_n$ is a transitive subgroup which contains a 3-cycle. Then all closed index n subgroups are conjugate if $n = p$ or $2p$ for some prime p.*

Proof. (a) Let $H \subseteq G$ be a nontransitive subgroup of index n and let $m_1, \ldots, m_s$ denote the lengths of the H-orbits of $[n] = \{1, \ldots, n\}$. Then $s \geqslant 2$, and we may assume $m_i \geqslant 2$ for all i. But then $|H| \leqslant m_1! \cdot \cdots \cdot m_s! \leqslant 2!(n-2)!$ is seen to rule out his possibility. Therefore $m_i = 1$ for some i.

(b) Let $n \geqslant 3$ be a positive integer and suppose $G \subseteq S_n$ is a transitive subgroup which contains a 3-cycle. We will call a subset $\mathscr{U} \subseteq [n]$ with at least three elements *3-closed* if for $a, b, c \in \mathscr{U}$ distinct $(abc) \in G$. One can check that if $\mathscr{U}$ and $\mathscr{U}'$ are 3-closed then $\mathscr{U} \cap \mathscr{U}' = \varnothing$ or $\mathscr{U} \cup \mathscr{U}'$ is 3-closed. (This reduces to the easy case where $\mathscr{U}$ and $\mathscr{U}'$ have three elements.) From ${}^{\tau}(abc) = (\tau a\, \tau b\, \tau c)$ we see that the maximal 3-closed subsets $\mathscr{U}_1, \ldots, \mathscr{U}_s$ partition $[n]$ and are permuted by $\tau \in G$. In particular $s \mid n$ and there is an induced representation $\pi: G \to \mathrm{Sym}(\tilde{X})$ where $\tilde{X}$ is the collection of maximal 3-closed sets.

If $n = p$, then $s = 1$ and thus $G = A_p$ or S_p. Assume H is any subgroup of index p. Then H is not transitive, otherwise $[H: G_1 \cap H] = p$ means $p^2 \mid\mid |G| \mid\mid p!$, a contradiction. Thus for $n = p$ all index n subgroups of G are conjugate by (a). If $n = 2p$, again by (a) we may assume $s = 2$, in which case $\mathscr{U}_1$ and $\mathscr{U}_2$ have p elements. Since $p \geqslant 3$ and $p \mid |G_1|$, necessarily $p \mid |H|$ and any element $\tau \in H$ of order p is in $\ker \pi$. Thus $\mathscr{U}_1$ or $\mathscr{U}_2$ is contained in an H-orbit of $[n]$, so we may assume $\mathscr{U}_1$ is an H-orbit. This means $H \subseteq \ker \pi$. Consider the restriction $\mathrm{res}: \ker \pi \to \mathrm{Sym}(\mathscr{U}_2) = S_p$. Since $\ker(\mathrm{res.}) \subseteq H$ we have $[\mathrm{Im}(\mathrm{res.}): \mathrm{res.}(H)] = [\ker \pi: H] = p$ since $[G: \ker \pi] = 2$. Thus by the preceding paragraph res.(H) stabilizes a point of $\mathscr{U}_2$. Q.E.D.

2.11. *Suppose $G \subseteq \mathrm{Aut}_k(V)$ is a subgroup as above and $u, w \in V$ are G-orbit basis generators.*

(a) *If G is generated by involutions a and b, then G_u and G_w are conjugate.*

(b) *Suppose $G_w(u)$ has two elements and $G_u G_w$ generates a dense subgroup of G. Then G_u and G_w are conjugate.*

(c) *Suppose $n = 2p$ for some prime p. Then some G_w-orbit of $G(u)$ does not have two elements.*

Proof. (a) $c = ab$ generates a normal subgroup $L = (c)$ of index 1 or 2 in G. Since $G_u \cap L$ is normal, $G_u \cap L = (e)$, so we may assume $|G_u| = 2$. Since ${}^{c}x = c^2 x$ for $x \notin L$, we may assume $G_u = (a)$ and $G_w = (b)$. From

$G = (c^2)\, G_u\, G_u$ and Lemma 2.8(d) we conclude that $(c^2) \subseteq G$ is dense. Thus c has odd order, so a and b are conjugate.

(b) G_u, $G_u \subseteq N(G_u \cap G_u)$ by Lemma 2.8(b), so $G_u \cap G_u$ is normal by Lemma 2.8(c). Thus $G_u \cap G_u = (e)$. This means $|G_u| = |G_u| = 2$. Since $G_u G_u$ generates G we now apply (a).

(c) Assume all G_u-orbits of $G(u)$ have two elements. Then by (b) the subgroup L generated $G_u G_u$ is not dense, so L is closed and proper by Lemma 2.8(c). Thus L has index 2 or index p. If $[G:L] = 2$, then L has an element of order p, so L has two orbits of length p. The G_u-orbits partition the L-orbits, so $p = 2$. Thus $[G:L] = p$ in any case. Therefore $[L: G_u] = 2$, so $N(G_u) = G_u G_u = G_{\mathcal{O}_u}$ where $\mathcal{O}_u = G_u(u)$. Replacing u by $g(u)$ for $g \in G$ we calculate $N(G_u) = \bigcap_g G_{\mathcal{O}_{g(u)}} = G_u$ since G_u is closed, a contradiction.

Q.E.D.

It is worth noting that 2.11(b) implies:

2.12. *If $G_u(u)$ has two elements and G_u has two $G(u)$ orbits, then $n = 3$.*

By using Lemma 2.8(a, b), 2.10–2.12, and considering the possibilities for the G_u-orbits of $G(u)$, one can easily prove part (a) of the above proposition, and in case $n = 7$ conclude that if G_u is not conjugate to G_u, then $G \subseteq \mathrm{Sym}(G(u))$ has no 3-cycles, and G_u has $G(u)$-orbits of length three and four, which we denote by $\mathcal{O} = \{1, 2, 3\}$, and $\mathcal{O}' = \{a, b, c, d\}$, respectively. We may assume $u = 1$ and $\mathbf{a} = (123)(abc) \in G_u$. There is a $\tau \in G_u$ which moves d. Note that $({}^{\tau}\mathbf{a})\mathbf{a}$ or $({}^{\tau}\mathbf{a})\mathbf{a}^{-1}$ is an even permutation which fixes 1, 2, 3 and moves d. Thus one of $(ab)(cd)$, $\mathbf{a}(ab)(cd) = (bc)(ad)$, $\mathbf{a}(bc)(ad) = (ca)(bd)$ is in G_u, hence all are. Since $|G_1| = |G_u|$ and $|G_u| \mid 3!4!$, we conclude that G_1 has an element of order three and that $5 \nmid |G_1|$. Thus the calculations ${}^{(xy)(zw)}(23x)(yzw) = (23y)(xwz)$ and $(23x)(yzw)(23y)(xwz) = (2xy3z)(w)$ show that (up to permutation of 1–3 and a–d) $\mathbf{a} \in G_u$ and either $\mathbf{d} = (2ad)(3bc)$ or $\mathbf{e} = (2ad)(3cb)$ is in G_1. If $\mathbf{e} \in G_1$, then ${}^{(ab)(cd)}\mathbf{e} = (2bc)(3da) \in G_1$. The pair $\mathbf{a}' = (132)(acb)$ and $\mathbf{d}' = (3ad)(2cb)$ is of the same type as $\mathbf{a}$ and $\mathbf{d}$. *Thus we may assume* $\mathbf{a}$ *and* $\mathbf{d}$ *are in* G. Since $G_u \to S_4$ $(\tau \mapsto \tau|_{\mathcal{O}'})$ is injective (G has no 3-cycles), the order of G is at most $7 \cdot 3 \cdot 8$. Let $\tau = \mathbf{da}$. Then τ is a 7-cycle. If G is any group with subgroups L, $H \subseteq G$, then $LH \subseteq G$ is a subgroup if $Lh \subseteq HL$ for generators h of H. Therefore the following computations show that G is generated by $\mathbf{a}$ and $\mathbf{d}$ and has order $7 \cdot 3 \cdot 8$: $\tau\mathbf{d}\tau^2 = (23)(ab) \equiv \mathbf{b}$, $\tau\mathbf{b}\tau^4 = (23)(acbd) \equiv \mathbf{c}$, $\tau\mathbf{c}\tau^4 = \mathbf{d}^{-1}$, $\tau\mathbf{d}^{-1}\tau^5 = \mathbf{c}^{-1}$, $\tau\mathbf{c}^{-1}\tau^4 = \mathbf{bc}^{-1}$, $\tau\mathbf{bc}^{-1}\tau^{-1} = \mathbf{cd}$, $\tau(\mathbf{cd})\,\tau^3 = \mathbf{d}$; $\mathbf{dbd}^{-1} = \mathbf{c}^2$, $\mathbf{dc}^2\mathbf{d}^{-1} = \mathbf{bc}^2$, $\mathbf{dbc}^2\mathbf{d}^{-1} = \mathbf{b}$, $\mathbf{dcd} = \mathbf{c}^{-1}$, $\mathbf{dc}^{-1}\mathbf{d} = \mathbf{bc}$, $\mathbf{dbcd} = \mathbf{c}$, and $\mathbf{bcb}^{-1} = \mathbf{c}^{-1}$.

One can easily realize G as $GL_3(Z_2)$ as follows. Let V be the vector space

over Z_2 with basis 1, 2, and a. Defining $1+2=3$, $1+a=b$, $2+a=c$, and $3+a=d$ one can easily check that **a** and **d** are linear. As $GL_3(Z_2)$ has $7\cdot 6\cdot 4$ elements, we have $G=GL_3(Z_2)$. Observe that a maximal closed subgroup of G has the form $G_{U\backslash 0}$ for some subspace $U\subseteq V$. Thus $G_\omega = G_{U\backslash 0}$ for some codimension 1 subspace $U\subseteq V$, and this means there are at most two conjugacy classes of stabilizers G_u of G-orbit basis generators.

Suppose, more generally, that $G(u)=V\backslash 0$, where V is a vector space over Z_2 of dimension $n\geqslant 3$, and make the natural identification $G\subseteq GL_n(Z_2)$ as above. Let $U\subseteq V$ be a subspace of codimension 1 and set $P=U\backslash 0$. Then G_p has two orbits, namely, P and $P^c=V\backslash U$. Thus $N(G_P)=G_P$, which means that $[G:G_P]=2^n-1=[G:G_u]$ since $[G:N(G_p)]$ is the number of conjugates of G_U (or the number of codimension one subspaces of V) and $[G:G_u]$ is the number of one-dimensional subspaces of V. Suppose $G_P=G_\omega$. Then $\omega=\alpha v_p+\beta v_{p^c}$ for some $\alpha,\beta\in k$. (For a non-void subset $S\subseteq V$ we define $v_S=\sum_{v\in S} v$.) Choose representatives $g_v\in G_\omega$ $(v\in V\backslash 0)$ for the left cosets of G_ω, and consider the matrix $A\in M(2^n-1,k)$ of $v\mapsto g_v(\omega)$ (order $V\backslash 0$ in some fashion). Observe that $g_v(\omega)=\alpha v_{g_v(P)}+\beta v_{g_v(P^c)}$. Write $A^tA=(a_{v,v'})$. Then one compute directly that

$$a_{v,v'}=\begin{cases}(2^{n-1}-1)\,\alpha^2+(2^n-2^{n-1})\,\beta^2 & \text{if } v=v'\\ (2^{n-2}-1)\,\alpha^2+2(2^{n-1}-2^{n-2})\,\alpha\beta+2^{n-2}\beta^2 & \text{if } v\neq v'.\end{cases}$$

If $B\in M(n+1,k)$ is a matrix whose entries satisfy $b_{ij}=\delta_{ij}x+(1-\delta_{ij})y$, then $\det B=(x-y)^n(x+ny)$ follows by induction. Thus if ω is a G-orbit basis generator, necessarily $\operatorname{char} k\neq 2$. If $\operatorname{char} k\neq 2$, setting $\alpha=1$ and $\beta=-1$ we compute $\det A^tA=(2^n)^{(2^n-2)}$, so ω is a G-orbit basis generator. This completes the proof of the proposition. Q.E.D.

2.13. THEOREM. *Let E be a finite-dimensional separable extension of an infinite field k of characteristic $p>0$. Then $\mathscr{L}(E)$ determines E if $[E:k]\leqslant 6$. If $[E:k]=7$, $\mathscr{L}(E)$ does not determine E if and only if $p>2$ and $G(\Omega\backslash k)\simeq GL_3(Z_2)$, where Ω is a splitting field of E over k. In this case are two isomorphism classes of algebras U with $\mathscr{L}(E)\simeq\mathscr{L}(U)$.*

Further analysis of $GL_n(Z_2)$ will show that there are two conjugacy classes of index 2^n-1 subgroups. The argument for $GL_n(Z_2)$ can be modified to suit other finite projective groups.

3. THE MAIN RESULTS

In this section we consider the cofree irreducible Hopf algebra $\mathrm{CH}(E)$ on a finite-dimensional separable extension of a field k of characteristic $p>0$.

Generally $\mathscr{L}(E)$ does not determine $\mathrm{CH}(E)$ and $\mathrm{CH}(E)$ does not determine E.

Suppose U is an algebra over k. The recall from Section 1 that $\mathfrak{F} = \mathrm{Aut}_k(U)$ acts on $\mathrm{CH}(U)$ as Hopf algebra automorphisms. Let $G(U, m)$ denote the group $\mathrm{Alg}_k(\langle \mathrm{CH}(U)_m \rangle, k)$ under the convolution multiplication $*$, and for a map $f: \mathrm{CH}(U) \to V$ let $f_{(m)} = f|_{\langle \mathrm{CH}(U)_m \rangle} \cdot G(U, m)$ is a right $\mathfrak{F}$-module ($\eta \cdot \sigma = \eta \circ \sigma_{(m)}$ for $\eta \in G(U, m)$ and $\sigma \in \mathfrak{F}$), and the rule $(\eta * \eta') \circ \sigma_{(m)} = (\eta \circ \sigma_{(m)}) * (\eta' \circ \sigma_{(m)})$ means that $\mathfrak{F}$ acts on $G(U, m)$ as group automorphisms. Clearly $\mathfrak{F}$ acts on $G(U, \infty) = \mathrm{Alg}_k(\mathrm{CH}(U), k)$ in the same manner.

Now suppose Ω is a splitting field of E over k and suppose $u \in E$ generates $\mathscr{L}(E)$. Let $B \subseteq \Omega$ be the conjugates of u, and for $a \in B$ set $p_a(X) = \prod_{b \in B \setminus a}((X - b)/(a - b))$. Observe that $X = \sum_a a p_a(X)$. Observe that $E \otimes_k \Omega$ is split and the $u_a = p_a(u \otimes 1)$'s constitute $\mathscr{E}$. For $\sigma \in G(\Omega \backslash k)$ we note that $\sigma(u_a) = u_{\sigma a}$ for $u_a \in \mathscr{E}$, so there is a natural identification of $G(\Omega \backslash k)$ with a subgroup of $\mathrm{Aut}_\Omega(E \otimes_k \Omega)$. Our first result shows that determining the isomorphism classes of $\mathrm{CH}(E)$ involves an extension problem.

3.1. PROPOSITION. *Let E be a finite-dimensional separable field extension of an infinite field k of characteristic $p > 0$, and let Ω be a splitting field of E over k. Suppose U is a k-algebra.*

(a) *If $\mathrm{CH}(E) \simeq \mathrm{CH}(U)$, then $\mathscr{L}(E) \simeq \mathscr{L}(U)$. Thus U is isomorphic as a k-algebra to a field extension $F \subseteq \Omega$.*

(b) *Assume $k \subseteq F \subseteq \Omega$ is a field extension. Then $\mathrm{CH}(E) \simeq \mathrm{CH}(F)$ if and only if there exists an F'-invariant $\eta \in G(E \otimes_k \Omega, \infty)$ such that $\alpha = \sum_a \eta(u_a) a \in V(u, \Omega \backslash k)$ is a $G(\Omega \backslash k)$-orbit basis generator ($\eta(u_a) \in Z_p$ necessarily) and $G(\Omega \backslash k)_\alpha = F'$.*

Proof. (a) $\mathrm{CH}(E) \simeq (\mathrm{CH}(U)$ implies $\mathscr{L}(E) \simeq \mathscr{L}(U)$ in any case. The remainder follows by Lemma 2.2 and Proposition 2.6.

(b) ($\Rightarrow$) Assume $f: \mathrm{CH}(E) \to \mathrm{CH}(F)$ is an isomorphism of Hopf algebras. Let $\mathrm{can.}: \mathrm{CH}(E) \otimes_k \Omega \simeq \mathrm{CH}(E \otimes_k \Omega)$ be the canonical isomorphism and define $\eta: \mathrm{CH}(E \otimes_k \Omega) \to \Omega$ by $\eta = m \circ (\pi \otimes I) \circ (f \otimes I) \circ \mathrm{can.}^{-1}$ where $m: F \otimes_k \Omega \to \Omega$ is multiplication and $\pi: \mathrm{CH}(F) \to F$ is the projection. Since $f|_E: E \to F$ is a Lie isomorphism, $f(u) \in V(u, \Omega \backslash k)$ and is $G(\Omega \backslash k)$-orbit basis generator by Proposition 2.5(b). But from $u \otimes 1 = \sum_a a p_a(u \otimes 1) = \sum_a a u_a$ we have $\alpha = f(u) = \eta(u \otimes 1) = \sum_a \eta(u_a) a$. Thus it follows $G(\Omega \backslash k)_\alpha = F'$. Since $G(\Omega \backslash k)_\eta \subseteq G(\Omega \backslash k)_\alpha$ and $F \simeq G(\Omega \backslash k)'_\eta$ by Proposition 1.11(c) we have that $G(\Omega \backslash k)_\eta = G(\Omega \backslash k)_\alpha = F'$, so η is F'-invariant.

($\Leftarrow$) Let $\eta \in G(E \otimes_k \Omega, \infty)$ be such an extension, and let $f: \mathrm{CH}(E) \to \Omega$ be the composite $f = \eta \circ (\text{can.}) \circ i$, where $i: \mathrm{CH}(E) \to \mathrm{CH}(E) \otimes \Omega$ is the natural inclusion. Then $f(u) = \eta(u \otimes 1) = \sum_a \eta(u_a)a \in V(u, \Omega \backslash k)$ is a $G(\Omega \backslash k)$-orbit basis generator by assumption. Thus $f|_E: E \to k[f(u)]$ is a Lie isomorphism. Thus from $G(\Omega \backslash k)'_u = F$ we conclude that $F = k[f(u)]$, so $\mathrm{CH}(E)/\ker f \simeq G'_\eta \subseteq F$ means $\mathrm{Im}\, f = F$. Therefore the restriction $f: \mathrm{CH}(E)^+ \to F$ is a multiplicative k-linear map such that $f|_E: E \to F$ is bijective. By [3, Lemma 3.1] we conclude that $\mathrm{CH}(E) \simeq \mathrm{CH}(F)$. Q.E.D.

Suppose that U is a split commutative algebra over a field k of characteristic $p > 0$ and $\mathscr{E}$ is the orthogonal basis of U. There is a natural identification of groups $\mathrm{Sym}(\mathscr{E}) = \mathrm{Aut}_k(U)$. For $\sigma \in \mathrm{Sym}(\mathscr{E})$ recall that the induced Hopf algebra automorphism $\boldsymbol{\sigma}$ of $\mathrm{CH}(U)$ is determined by $\boldsymbol{\sigma}(u_1 \otimes \cdots \otimes u_n) = \sigma(u_1) \otimes \cdots \otimes \sigma(u_n)$ for $u_1, \ldots, u_n \in \mathscr{E}$. Suppose $G \subseteq \mathrm{Sym}(X)$ is a subgroup. For a G-orbit $\mathscr{O} \subseteq X$ the restriction map res.: $G \to \mathrm{Sym}(\mathscr{O})$ is a group homomorphism. Set $\mathrm{res.}(G) = G_{(\mathscr{O})}$.

3.2. LEMMA. *Suppose U is a split commutative algebra over a field k of characteristic $p > 0$ with orthogonal basis $\mathscr{E}$. Let $G \subseteq \mathrm{Sym}(\mathscr{E})$ be a subgroup and $\eta \in G(U, \infty)$ be G-invariant. If $\mathscr{O} \subseteq \mathscr{E}$ is a G-orbit and $p \,|\, |G_{(\mathscr{O})}|$, then $\eta(\mathscr{O}) = (0)$.*

Proof. Since $p \,|\, |G_{(\mathscr{O})}|$, there are $u_1, \ldots, u_p \in \mathscr{O}$ and a $\sigma \in G$ of the form $\sigma = (u_1 \cdots u_p) \circ \tau$, where $\tau \in \mathrm{Sym}(\mathscr{E})$ fixes the u_i's. By [3, § 1] we compute in $\mathrm{CH}(U)$ that $u_1 \circ \cdots \circ u_p = \sum_\alpha u_{\alpha 1} \otimes \cdots \otimes u_{\alpha p}$, where α runs over S_p. Since the $u_{\alpha 1} \otimes \cdots \otimes u_{\alpha p}$'s split up into $(\boldsymbol{\sigma})$-orbits of length p, and $\eta \circ \boldsymbol{\sigma} = \eta$, we compute $\eta(u_1 \circ \cdots \circ u_p) = 0$. But η is constant on G-orbits, so $\eta(u_1) = \eta(u_1)^p = \eta(u_1 \circ \cdots \circ u_p) = 0$. This means $\eta(\mathscr{O}) = (0)$. Q.E.D.

The first theorem in this section shows that $\mathscr{L}(E)$ does not generally determine $\mathrm{CH}(E)$ where E is a separable field extension. The examples we produce are motivated by the combination of Proposition 3.1 and Lemma 3.2. The crux of the proof is:

3.3. LEMMA. *Let k be an infinite field of characteristic $p > 0$, let E be a finite-dimensional separable extension of k, and suppose Ω is a splitting field of E over k. Suppose $u \in E$ generates $\mathscr{L}(E)$ and $\omega \in V(u, \Omega \backslash k)$ is a $G(\Omega \backslash k)$-orbit basis generator, and set $F = k[\omega]$. Then $\mathscr{L}(E) \simeq \mathscr{L}(F)$, and if $p \| (G_\omega)_{(\mathscr{O})}|$ for all G_ω-orbits $\mathscr{O}$ of $G(u)$, then $\mathrm{CH}(E) \not\simeq \mathrm{CH}(F)$.*

3.4. THEOREM. *Let p be any positive prime integer. There exists a field k of characteristic p and finite-dimensional separable field extensions E, F of k such that $\mathscr{L}(E) \simeq \mathscr{L}(F)$ but $\mathrm{CH}(E) \not\simeq \mathrm{CH}(F)$.*

Proof. Let X be a non-void finite set and let $G \subseteq \mathrm{Sym}(X)$ be a subgroup. Regard G as automorphisms of the function field $\Omega = Z_p(X)$ and let $k \subseteq \Omega$ be the fixed field of G. Then $G = G(\Omega \backslash k)$, and for $u \in X$ it follows that $k[u]$ is a finite-dimensional separable extension of k, and Ω is the splitting field of $k[u]$ over k if G is transitive. Assume G is transitive. For $u \in X$ we conclude that u generates $\mathscr{L}(k[u])$, since $G(u) = X$ is a set of indeterminants over Z_p.

First assume $n > p > 2$ and let V be an n-dimensional vector space over Z_2. Let $X = V \backslash 0$ and regard $G = GL_n(Z_2)$ as a subgroup of $\mathrm{Sym}(X)$ in the natural way. Let $U \subseteq V$ be a codimension one subspace and choose $u \notin U$. For $P = U \backslash 0$ we showed at the end of the proof of Proposition 2.9 that $\omega = v_p - v_p^c \in V(u, \Omega \backslash k)$ is a $G(\Omega \backslash k)$-orbit basis generator and that G_ω has $G(u) = X$-orbits P and P^c. Let $a_1, \ldots, a_p \in U$ be independent and choose $\tau \in G_u \cap G_\omega$ which extends the p-cycle $(a_1, \ldots, a_p)$. Then $(a_1 + u, \ldots, a_p + u)$ is also a cycle in the cyclic decomposition of τ, so by Lemma 3.3, $\mathscr{L}(E) \simeq \mathscr{L}(F)$ but $\mathrm{CH}(E) \not\simeq \mathrm{CH}(F)$, where $E = k[u]$ and $F = k[\omega]$.

We give a degree 11 example for $p = 2$. Let $X = [11]$ and a–f represent 6–11 in order, and let $G \subseteq S_{11}$ be the subgroup generated by $\mathbf{a} = (12534)(bcdef)$ and $\mathbf{d} = (23abc)(4d5ef)$. Then $\tau = \mathbf{da}$ is an 11-cycle, and as at the end of the proof of Proposition 2.9 the following calculations show that G has order $11 \cdot 5 \cdot 3 \cdot 4$. Let $\mathbf{b} = (345)(aeb)(cfd)$ and $\mathbf{c} = (325)(cbe)(adf)$.

$\tau \mathbf{d} \tau^3 = \mathbf{db}^{-1}$, $\tau \mathbf{db}^{-1} \tau^2 = \mathbf{d}^3 \mathbf{b}$, $\tau \mathbf{d}^3 \mathbf{b} \tau^{-1} = \mathbf{dc}$, $\tau \mathbf{dc} \tau^2 = \mathbf{d}^{-1} \mathbf{bc}^{-1}$, $\tau \mathbf{d}^{-1} \mathbf{c}^{-1} \tau^6 = \mathbf{b}$, $\tau \mathbf{b} \tau = \mathbf{b}^{-1}$, $\tau \mathbf{b}^{-1} \tau^5 = \mathbf{d}^{-1}$, $\tau \mathbf{d}^{-1} \tau^2 = \mathbf{d}^3 \mathbf{c}^{-1}$, $\tau \mathbf{d}^3 \mathbf{c}^{-1} \tau = \mathbf{cd}^2$, $\tau \mathbf{cd}^2 \tau^9 = \mathbf{d}^{-1} \mathbf{c}^{-1}$, $\tau \mathbf{d}^{-1} \mathbf{c}^{-1} \tau^3 = \mathbf{d}$;

$\mathbf{dbd}^{-1} = \mathbf{bc}^{-1}$, $\mathbf{dbc}^{-1} \mathbf{d}^2 = \mathbf{cb}$, $\mathbf{dcbd}^2 = \mathbf{b}^{-1}$, $\mathbf{db}^{-1} \mathbf{d}^{-1} = \mathbf{cb}^{-1}$, $\mathbf{dcb}^{-1} \mathbf{d}^3 = \mathbf{b}$; $\mathbf{dcd} = \mathbf{c}^{-1}$, $\mathbf{dc}^{-1} \mathbf{d}^2 = \mathbf{b}^{-1} \mathbf{c}$, $\mathbf{db}^{-1} \mathbf{cd} = \mathbf{c}^{-1} \mathbf{b}$, $\mathbf{dc}^{-1} \mathbf{bd}^3 = (\mathbf{bc})(\mathbf{cb})$, $\mathbf{d}(\mathbf{bc})(\mathbf{cb})\, \mathbf{d}^3 = \mathbf{c}$;

$\mathbf{bc} = (23)(45)(ac)(ef)$ and $\mathbf{cb} = (25)(34)(ac)(bd)$ generate $H \simeq Z_2 \times Z_2$. (This means $\mathbf{b}$ normalizes H.)

Let $P = \{1, \ldots, 5\}$ and $P^c = \{a, \ldots, f\}$. Then

$$\mathbf{a}, \mathbf{b}, \mathbf{c} \quad \text{generate} \quad G_P \simeq A_5,$$

$$\mathbf{d}, \mathbf{b}, \mathbf{c} \quad \text{generate} \quad G_1 \simeq A_5,$$

G (order $11 \cdot 5 \cdot 3 \cdot 4$) generated by $\mathbf{a}$ and $\mathbf{d}$.

Observe that $G_P = G_\omega$ where $\omega = v_P$. If $\tau^l(P) \neq \tau^{l'}(P)$, then $\tau^l(P) \cap \tau^{l'}(P)$ has two elements, so one can mimic the argument for $GL_n(Z_2)$ at the end of the proof of Proposition 2.9 to show that $\omega \in V(u, \Omega \backslash k)$ is a $G(\Omega \backslash k)$-orbit basis generator ($u = 1$) for $p = 2$. As $\mathbf{bc} = (23)(45)(ac)(ef) \in G_\omega$ we apply Lemma 3.3 to $E = k[u]$ and $F = k[\omega]$. Q.E.D.

Remark. By virtue of Theorem 2.13, the example above for $p = 2$, and the fact that any finite group can be realized as a Galois group, $\mathscr{L}(E)$ does not determine E in any characteristic.

The second theorem in this section gives a sufficient condition for $\mathscr{L}(E)$ to determine $\mathrm{CH}(E)$. The heart of the proof is part (b) of the following result.

3.5. PROPOSITION. *Suppose that U is a finite-dimensional commutative split algebra over a field of characteristic $p > 0$ and $G \subseteq \mathfrak{F} \subseteq \mathrm{Aut}_k(U)$ is a subgroup.*

(a) *If all G-invariant $\eta_0 \in G(U, 1)$ have a G-invariant extension $\eta \in G(U, \alpha)$, then $p \nmid |G|$.*

(b) *Suppose $p \nmid |G|$ and G is solvable. Then if $n \geqslant 1$, every G-invariant $\eta_0 \in G(U, n)$ has a G-invariant extension $\eta \in G(U, \infty)$.*

Proof. (a) Let $\eta_0 \in G(U, 1)$ be defined by $\eta_0(u_1) = \cdots = \eta_0(u_n) = 1$, where $\mathscr{B} = \{u_1, \ldots, u_n\}$ is the orthogonal basis of U. If $\eta \in G(U, \infty)$ is a G-invariant extension of η_0, then by Lemma 3.2 and hypothesis $p \nmid |G_{(\mathscr{O})}|$ for all G-orbits $\mathscr{O} \subseteq \mathscr{B}$, so $p \nmid |G|$.

(b) Assume $p \nmid |G|$; and let $\eta_0 \in G(U, n)$ be G-invariant. We need only show that η_0 has a G-invariant extension $\eta \in G(U, n + 1)$. This we will do by induction on $|G|$. The case $|G| = 1$ follows by Proposition 1.6. Suppose $|G| > 1$. Since G is solvable, G has a normal subgroup H such that G/H has prime order q. By assumption $q \neq p$. Let $G_H(U, m) \subseteq G(U, m)$ be the H-invariants of $G(U, m)$. Then since $\mathfrak{F}$ acts on $G(U, m)$ as group automorphisms, $G_H(U, m)$ is a subgroup of $G(U, m)$. Since H is normal, $G_H(U, m)$ is also a G-submodule of $G(U, m)$. Now the restriction map $r_m: G(U, m + 1) \to G(U, m)$ is a $\mathfrak{F}$-module map as well as a group homomorphism. Thus $r_m(G_H(U, m + 1)) \subseteq G_H(U, m)$, and by induction the induced map $\mathbf{r}_n: G_H(U, n + 1) \to G_H(U, n)$ is surjective.

Suppose $\eta_0 \in G(U, n)$ is G-invariant. Then $\eta_0 \in G_H(U, n)$, and the subset $X \subseteq G_H(U, n + 1)$ of extensions of η_0 is a coset of $\ker \mathbf{r}_n$ and a G-submodule. But $|G(U, m)| = \dim\langle \mathrm{CH}(U)_m \rangle$ is a power of p for any $m \geqslant 1$ by Proposition 1.7(b), so $|X| = p^l$ for some $l \geqslant 0$. Since $\eta \cdot G$ has 1 or q elements whenever $\eta \in X$, necessarily some $\eta \in X$ must be G-invariant. This concludes the proof of (b). Q.E.D.

Let E be a finite-dimensional separable extension of a field k of characteristic $p > 0$, and let Ω be a splitting field of E over k. Then E is called *residually solvable* if E' is a solvable subgroup of $G(\Omega \backslash k)$.

3.6. THEOREM. *Let E be a finite-dimensional residually solvable extension of a field k of charcteristic $p > 0$, and suppose $p \nmid |E'|$. Then $\mathscr{L}(E)$ determines* $\mathrm{CH}(E)$.

Proof. We may assume that k is infinite. Let F be a k-algebra and suppose $\mathscr{L}(E) \simeq \mathscr{L}(F)$. Then we may assume F is a field extension of k and $k \subseteq F \subseteq \Omega$, where Ω is a splitting field of E over k. By Proposition 2.6, Ω is a splitting field of F over k. Let u generate $\mathscr{L}(F)$. Then $E = k[\omega]$, where $\omega \in V(u, \Omega\backslash k)$ is a $G(\Omega\backslash k)$-orbit basis generator, by Proposition 2.5. Write $\omega = \sum_a \alpha_a a$ where a runs over $G(\Omega\backslash k)(u)$ and $\alpha_a \in Z_p$. Since $\mathrm{Map}(\mathscr{E}, Z_p) = \mathrm{Alg}_\Omega(U, \Omega)$ by Proposition 1.7(a), there exists an $\eta_0 \in (F \otimes_k \Omega, 1)$ such that $\eta_0(u_a) = \alpha_a$ for all a. Since $E' \simeq G(\Omega\backslash k)_\omega = G(\Omega\backslash k)\eta_0$, η_0 is E'-invariant, so by Proposition 3.5(b) η_0 has an E'-invariant extension $\eta \in G(F \otimes_k \Omega, \infty)$. Thus $\mathrm{CH}(F) \simeq \mathrm{CH}(E)$ follows by Proposition 3.1(b). Q.E.D.

The condition $p \nmid |E'|$ cannot be dropped. To see this consider Proposition 2.9(b) and Lemma 3.3 when $p = 3$.

3.7. COROLLARY. *Let E be an n-dimensional separable field extension of an infinite field k of characteristic $p > 0$, and suppose U is a k-algebra. Then* $\mathrm{CH}(E) \simeq \mathrm{CH}(U)$ *implies* $E \simeq U$ *if* $n \leqslant 6$. *If* $n = 7$, $\mathrm{CH}(E)$ *does not determine E if and only if* $p > 3$ *and* $G(\Omega\backslash k) \simeq GL_3(Z_2)$, *where Ω is a splitting of E over k.*

Proof. Suppose $\mathrm{CH}(E) \simeq \mathrm{CH}(U)$. Then by Proposition 3.1(a) we may assume $U = F$ is a field such that $k \subseteq F \subseteq \Omega$ and $\mathscr{L}(E) \simeq \mathscr{L}(F)$. By Theorem 2.13, $\mathrm{CH}(E)$ determines E if $n \leqslant 6$. If $n = 7$ and $\mathrm{CH}(E) \simeq \mathrm{CH}(F)$ but $E \not\simeq F$, by the same result $G(\Omega\backslash k) \simeq GL_3(Z_2)$ and $p > 2$. One can use Lemma 3.3 to show $\mathrm{CH}(E) \not\simeq \mathrm{CH}(F)$ if $p = 3$, so $p > 3$ in fact. Conversely, if $p > 3$ and $G \simeq GL_3(Z_2)$, then Theorem 3.6 applies to $E' \simeq S_4$, so in this case we now use Proposition 3.1 to show $\mathrm{CH}(E)$ does not determine E. Q.E.D.

By virtue of Propositions 3.1 and 2.5 and Lemma 3.3:

3.8. COROLLARY. *Let k be a field of characteristic $p > 0$ and suppose that E is a finite-dimensional separable field extension of k. If E' is a p-group, then* $\mathrm{CH}(E)$ *determines E as a k-algebra.*

ACKNOWLEDGMENTS

The author would like to thank Professor Noboru Ito for several helpful discussions during the course of the research for this paper. Also this paper was revised during the time the author was on leave at Rutgers University. He wishes to express appreciation for the institution's hospitality.

REFERENCES

1. N. BOURBAKI, "Elements de Mathematique XI," Hermann, Paris, 1959.
2. I. KAPLANSKY, "Fields and Rings," Univ. of Chicago Press, Chicago, 1979.
3. K. NEWMAN AND D. E. RADFORD, The cofree irreducible Hopf algebra on an algebra, *Amer. J. Math.* **101**, No. 5, 1025–1045.
4. D. PASSMAN, "Permutation Groups," Benjamin, New York, 1968.
5. D. E. RADFORD, A natural ring basis for the shuffle algebra and an application to group schemes, *J. Algebra* **58**, No. 2 (June 1979), 432–454.
6. M. E. SWEEDLER, "Hopf Algebras," Benjamin, New York, 1969.